Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A validation protocol for determining authenticity of a printer consumable, said protocol including the steps of:

providing a printer containing a trusted authentication chip and a printer consumable containing an untrusted authentication chip;

generating a secret random number and calculating a signature for the random number using a signature function, in the trusted chip, the trusted chip having a random function to produce random numbers from a seed, and the function advances after each successful validation, so that the next random number is produced from a new seed;

encrypting the random number and the signature by a symmetric encryption function using a first key, in the trusted chip;

passing the encrypted random number and signature from the trusted chip to the untrusted chip;

decrypting the encrypted random number and signature with a symmetric decryption function using the first key, in the untrusted chip;

calculating a signature for the decrypted random number using the signature function, in the untrusted chip;

comparing the signature calculated in the untrusted chip with the signature decrypted, in the untrusted chip;

in the event that the two signatures match, in the untrusted chip, encrypting the decrypted random number by the symmetric encryption function using a second key and returning the encrypted random number to the trusted chip;

calling a test function in the trusted chip, the test function being called by the trusted chip first receiving, a plural and random number of times, a first number, then receiving the encrypted random number from the untrusted chip, the test function including:

encrypting the random number by the symmetric encryption function using the second key, in the trusted chip, to produce a second number;

comparing, up to said plural and random number of times, the ~~random number encrypted using the~~ second ~~key~~ number with the ~~respective~~ first number ~~or encrypted random number from the untrusted chip~~, in the trusted chip, the first

number being selected such that the comparison should never ~~returns~~ return a match ~~and~~in the trusted chip,

in the event that the current comparison with the first number returns a match, considering the trusted chip to be invalid and terminating the protocol;

in the event that all of the comparisons with the first number return a mismatch, comparing the second number with the encrypted random number from the untrusted chip ~~being produceable by the untrusted chip such that the comparison returns either a match or a mismatch~~, in the trusted chip;

in the event that the comparison with the encrypted random number from the untrusted chip returns a match, considering the untrusted chip to be valid and authorizing use of the printer consumable; and

in the event that the comparison with the encrypted random number from the untrusted chip returns a mismatch, considering the untrusted chip to be invalid and denying use of the printer consumable.

2. (Original) The protocol according to claim 1, where the first and second keys are held in both the trusted and untrusted authentication chips, and are kept secret.

3. (Cancelled)

4. (Original) The protocol according to claim 1, where the symmetric decrypt function is held only in the untrusted chip.

5. (Original) The protocol according to claim 1, where the signature function generates digital signatures of 160 bits.

6. (Cancelled)

7. (Original) The protocol according to claim 6, where the time taken to return an indication the chip is invalid is the same for all bad inputs, and the time taken to return the random number encrypted with the second key is the same for all good inputs.

8. (Original) The protocol according to claim 1, where a test function is held only in the trusted chip to advance the random number if the untrusted chip is valid; otherwise it returns an indication the chip is invalid.

9. (Original) The protocol according to claim 8, where the time taken to return an indication the chip is invalid is the same for all bad inputs, and the time taken to return an indication the chip is valid is the same for all good inputs.

10. (Original) The protocol according to claim 1, where it is used to determine the physical presence of a valid authentication chip.

11. (Previously Presented) A validation system for performing the method according to claim 1, where the system includes a printer containing a trusted authentication chip and a printer consumable containing an untrusted authentication chip; where the trusted authentication chip includes a random number generator, a symmetric encryption function and two keys for the function, a signature function and a test function; and the untrusted authentication chip includes a symmetric encryption and decryption function and two keys for these functions, a signature function, and a prove function to decrypt a random number and signature encrypted using the first key by the trusted authentication chip, and to calculate another signature from the decrypted random number, for comparison with the decrypted signature, and in the event that the comparison is successful to encrypt the random number with the second key and send the encrypted random number back; the test function in the trusted chip then operates to generate an encrypted version of the random number using the second key and to compare the encrypted random number with the received version to validate the untrusted chip, where the trusted authentication chip contains a random function to produce random numbers from a seed, and the function advances after each successful validation, so that the next random number will be produced from a new seed.

12. (Original) A validation system according to claim 11, where the remainder of the system is software, hardware or a combination of both, but the trusted chip is a physical authentication chip.

13. (Original) A validation system according to claim 11, where both chips have the same internal structure.

14. (Original) A validation system according to claim 11, where the first and second keys are kept secret.

15. (Cancelled)

16. (Original) A validation system according to claim 11, where the signature function generates digital signatures of 160 bits.

17. (Original) A validation system according to claim 11, where the prove function returns an indication the chip is invalid for all bad inputs and the time taken to do this is the same for all bad inputs, and the time taken to return the random number encrypted with the second key is the same for all good inputs.

18. (Original) A validation system according to claim 11, where the test function advances the random number if the untrusted chip is validated.

19. (Original) A validation system according to claim 11, where the time taken for the test function to return an indication the chip not validated is the same for all bad inputs, and the time taken to return an indication that the chip is validated is the same for all good inputs.

20. (Original) A validation system according to claim 11, where it is used to determine the physical presence of a valid authentication chip.